CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

DIANA CAROLINA JIMENEZ PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, D.C.
2022

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

DIANA CAROLINA JIMENEZ PARRA

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre
Luis Fernando Zambrano Hernandez
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C
2022

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

BLUE TEAM: Son equipos conformados para analizar e identificar las fallas de seguridad, validando que las actuales se encuentren vigentes.

DLP: Es un sistema, una herramienta que nos permite detectar según los parámetros configurados, fuga de información en la compañía, sea por medio de correo electrónico o por transferencias entre otras aplicaciones[1].

EXPLOIT: Son ataques que aprovechan las vulnerabilidades de la empresa, pueden ir desde las vulnerabilidades encontrada en las redes, aplicaciones, hardware, etc., por medio de programas o de códigos desarrollados para explotarlas. Los Exploit se clasifican en:

IDS: Un IDS es un sistema que permite detectar el ingreso no autorizado a los PC´s o a la red informando a los administradores emitiendo alertas o logs.

M**ETASPOTABILE3:** Es una maquina diseña para realizar pruebas de seguridad en un ambiente seguro.

1 LIU, Simon; KUHN, Rick. Data loss prevention. IT professional, 2010, vol. 12, no 2, p. 7

RESUMEN

El enfrentamiento de equipo rojo contra el equipo azul es una técnica de la ciberseguridad que nos permite evaluar la seguridad actual de una organización, logrando realizar bajo un escenario controlado, simulando técnicas de ataques verdaderas, pruebas de penetración dentro del perímetro de la red y así mismo la defensa y la capacidad de identificar, evaluar y responder oportunamente con el fin de encontrar las vulnerabilidades y debilidades que tiene la infraestructura y el personal dentro de la organización logrando así prepararse y mejorar los mecanismos de respuesta ante un ataque verdadero. El personal de seguridad de la información al realizar estas pruebas se valdrá de los conocimientos previos para realizar la explotación de las vulnerabilidades en todo el campo correspondiente.

Palabras clave: Análisis, ataques, pruebas, seguridad, vulnerabilidades.

ABSTRACT

The confrontation of the red team against the blue team is a cybersecurity technique that allows us to evaluate the current security of an organization, managing to perform under a controlled scenario, simulating real attack techniques, penetration tests within the perimeter of the network and thus The defense itself and the ability to identify, evaluate and respond in a timely manner in order to find vulnerabilities and weaknesses in the infrastructure and personnel within the organization, thus preparing and improving the response mechanisms to a real attack. When conducting these tests, information security personnel will use prior knowledge to exploit vulnerabilities in the entire corresponding field.

Keywords: analysis, attacks, testing, security, vulnerabilities.

INTRODUCCIÓN

Para un profesional de seguridad de TI, es importante identificar los impactos y especialmente las causas de los incidentes de seguridad mediante el análisis de escenarios, la investigación y la creación de pruebas de los laboratorios de construcción y ensamblaje, así como el uso de herramientas, entornos y las oportunidades pueden ser útiles para encontrar soluciones para abordar y mitigar las causas y efectos de las vulnerabilidades y amenazas que interrumpen el sustrato de información y, en muchos casos, pueden prevenir delitos informáticos ilícitos.

Hay variedad de fuentes confiables de información en las que se pueden consultar las nuevas vulnerabilidades, se deben consultar con frecuencia para obtener las amenazas a los que se enfrentan los sistemas informáticos indicando como mitigar y/o corregir la vulnerabilidad. Actualmente a la ciberseguridad no se le da el papel que se merece dentro de una organización, si durante un ataque se ven involucrados páginas webs primordiales para el funcionamiento de esta, servidores que sean vulnerados, bases de datos clonadas y otros incidentes de gran magnitud, las empresas solo suelen remediar esos daños, pero no buscan fortalecer la defensa para prevenir los mismos y estos es lo que se quiere llegar a implementar en todas las organizaciones. La finalidad de este análisis es poder brindad a las compañías

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Analizar el escenario controlado mediante el enfoque del RED TEAM & BLUE TEAM, con el fin de identificar las posibles amenazas y riesgos de seguridad a los que se encuentran expuestos y la forma de poder recudir el impacto de los ataques.

1.2 OBJETIVOS ESPECÍFICOS

- Ejecutar el banco de trabajo, para que por medio de este se permita el uso de herramientas de software libre que permitan gestionar los riesgos e identificar vulnerabilidades desde el enfoque del Red Team y Blue Team

- Demostrar las vulnerabilidades identificadas sobre el escenario controlado al aplicar las herramientas de software libre determinadas con el fin de mitigar el riesgo

- Establecer recomendaciones basadas estándares de buenas prácticas con el fin de gestionar el riesgo y mantener la confidencialidad, disponibilidad e integridad de la información desde la perspectiva del Blue Team.

2 DESARROLLO

2.1 ETAPA 1 - CONCEPTOS

En esta etapa se brinda una breve explicación de los conceptos básicos para ingresar al mundo del blue team y red team, conociendo lo fundamental en este campo e iniciando la comunicación entre las máquinas virtuales necesarias para el laboratorio a desarrollar.

2.1.1 Marco legal sobre delitos Informáticos

Una de la leyes que aplica , es la ley 1273 de 2009 ya que se acceden a los sistemas por medio de las pruebas de penetración, logrando adicional del ingreso, obtener información, modificarla y/o eliminarla, logrando obstaculizar el funcionamiento del sistema. Los artículos que más se aplican son los siguientes:

ARTÍCULO 269A. **Acceso abusivo a un sistema informático**.[2] Sin autorización acceder a sistemas protegidos o se mantenga en el sistema en contra de la voluntad.

ARTÍCULO 269B. Obstaculización ilegítima de sistema informático. Sin autorización obstaculice el funcionamiento normal del sistema.

ARTÍCULO 269C. Interceptación de datos informáticos. Sin autorización se capture datos informáticos del sistema.

ARTÍCULO 269D. Daño informático. Sin autorización el atacante acceda, destruya, modifique y/o elimine datos de los sistemas de información

[2] POLICIA NACIONAL DE COLOMBIA. [Sitio web]. Normatividad sobre delitos informáticos. [Consulta: 01 de septiembre 2022]. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

También se aplicaría la ley 1581 de 2012 ya que esta nos indica que está prohibida la transferencia de datos personales a países que no tengan un nivel de protección de datos adecuado, ya que este trabajo se puede llegar a topar con datos personales de los usuarios y es importante tenerlo en cuenta frente al marco legal. Los niveles adecuados son los estándares fijados por la superintendencia de industria y comercio del país[3].

2.1.2 Marco legal sobre delitos informáticos

El pentesting es una práctica que consiste en realizar una simulación de un ataque lo más verdadero posible en un entorno controlado establecido previamente con el objetivo de identificar fallas de seguridad de la organización para así ser corregidos a tiempo. Las principales fases del pentesting son:

Reconocimiento: En esta fase se recolecta toda la información a través de diversidad de técnicas como recopilación de metadatos, dominios, puertos, Google Dorks e información de terceros.

Análisis de vulnerabilidades: Según el resultado de la fase anterior, en esta etapa se analiza la información obtenida intentando buscar las vulnerabilidades, CVE a explotar.

Explotación: Es esta fase consiste en explotar todas las vulnerabilidades, comprobando que no se puedan ejecutar ataques como control de errores, inyección de código, evasión de autenticación, entre otros.

Post Explotación: Se deben realizar actividades de post explotación a las vulnerabilidades en los casos en donde estas puedan realizar diferentes acciones,

[3] SUPERINTENDECIA INDUSTRIA Y COMERCIO. . [Sitio web]. Protección de Datos Personales. [Consulta: 01 de septiembre 2022]. Disponible en: https://www.sic.gov.co/preguntas-frecuentes-pdp#:~:text=La%20Ley%201581%20de%202012%20proh%C3%ADbe%20la%20transferencia%20de%20datos,e%20inequ%C3%ADvoca%20para%20la%20transferencia.

algunas son como realiza acciones en los servidores, del lado de los usuarios, obtener información confidencial.

Informes: Es un documento indicando como se ha realizado el test de intrusión, que vulnerabilidades se han encontrado y la forma en la que pueden ser explotados.

2.1.3 Definición de herramientas

2.1.3.1 Herramientas

Metasploit: Es una herramienta que nos permite validar las vulnerabilidades de seguridad el cual es de código abierto y fue creada con la intención de ser utilizada por los auditores de seguridad y para este caso para las pruebas de los equipos de Blue y Red Team. Cuenta con varios módulos que contienen códigos para que se puedan explotar, por lo general estas vulnerabilidades son bastantes conocidas[4].

Nmap: Igual que metasploit, nmap es una aplicación de código abierto la cual nos permite escanear las redes y puertos de una organización logrando descubrir información importante con el fin de realizar auditorías. Con esta herramienta se puede mapear las redes, realizar auditorías, detección de sistemas operativos entre otros[5].

OpenVas: Es una herramienta que nos permite descubrir variedad de problemas a través de un scanner completo de las vulnerabilidades desde las de bajo riesgos como las más graves, esta herramienta surgió a partir de Nessus y es una herramienta que pertenece a la familia Greenbone. Con OpenVas se pueden utilizar

[4] OPEN WEBINARS. [Sitio web]. Qué es Metasploit framework. [Consulta: 02 de septiembre 2022]. Disponible en: https://openwebinars.net/blog/que-es-metasploit/
[5] HOSTING PLUS. [Sitio web]. Qué es Metasploit framework. [Consulta: 03 de septiembre 2022]. Disponible en: https://www.hostingplus.com.co/blog/que-es-nmap-y-para-que-sirve/

diferentes funciones como las pruebas autenticadas/no autenticadas, protocolos industriales y ajustes personalizados[6].

2.1.3.2 Servicios en línea

ExploitDB: Es un directorio en línea donde los hackers colaboran subiendo vulnerabilidades de aplicaciones y la forma de explotarlas indicando el paso a paso a seguir.

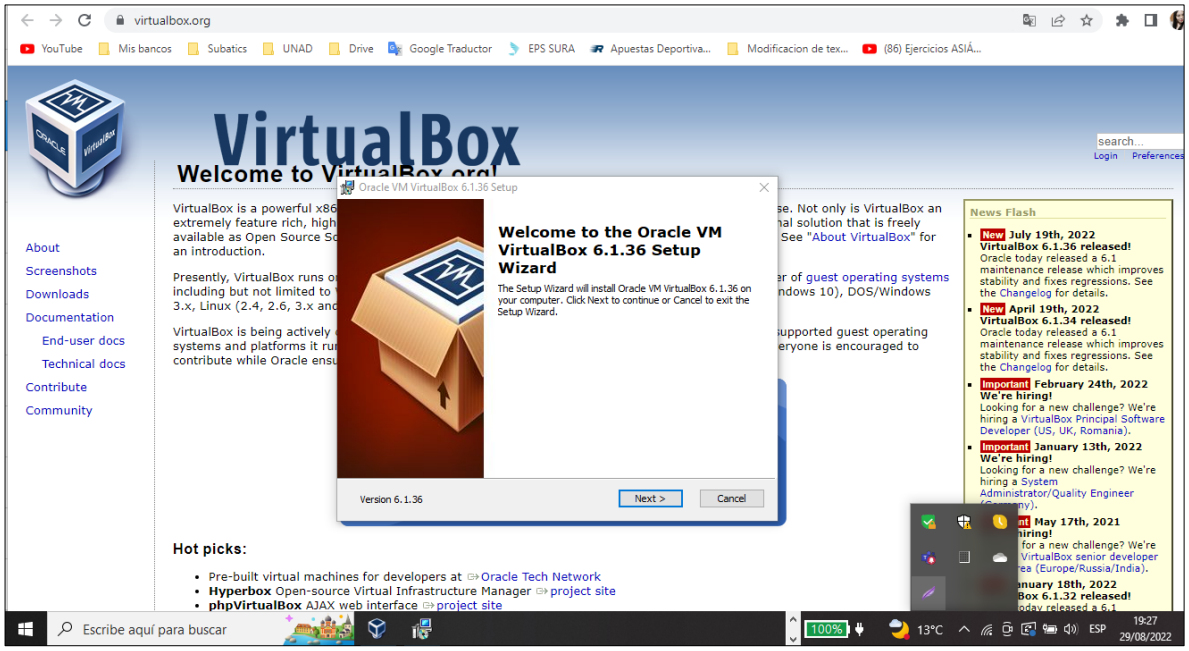
CVE: Es una numeración que se le da a las vulnerabilidades encontradas y con la cual se pueden identificar las mismas por media de una lista, un glosario que es divulgado al público.

2.1.4 Banco de trabajo

Paso A. Descargar VIRTUALBOX a la última versión.

[6] OPEN WEBINARS . [Sitio web]. Qué es OpenVas? [Consulta: 03 de septiembre 2022]. Disponible en: https://openwebinars.net/blog/que-es-openvas/

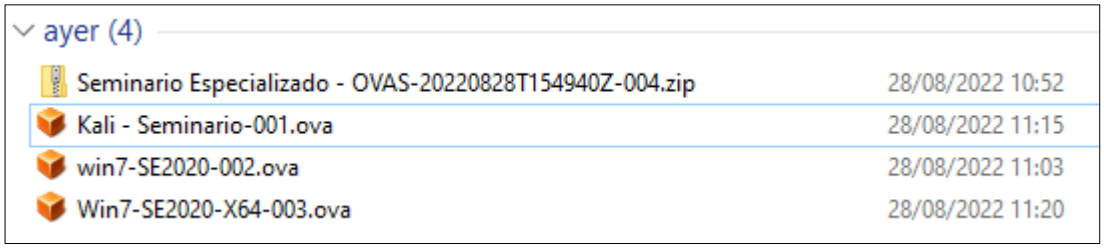
Figura 1. Descarga de la última versión.



Fuente 1. Elaboración propia

Paso B. Descargar las imágenes de las máquinas virtuales a trabajar.

Figura 2. Imágenes de las máquinas virtuales descargadas.

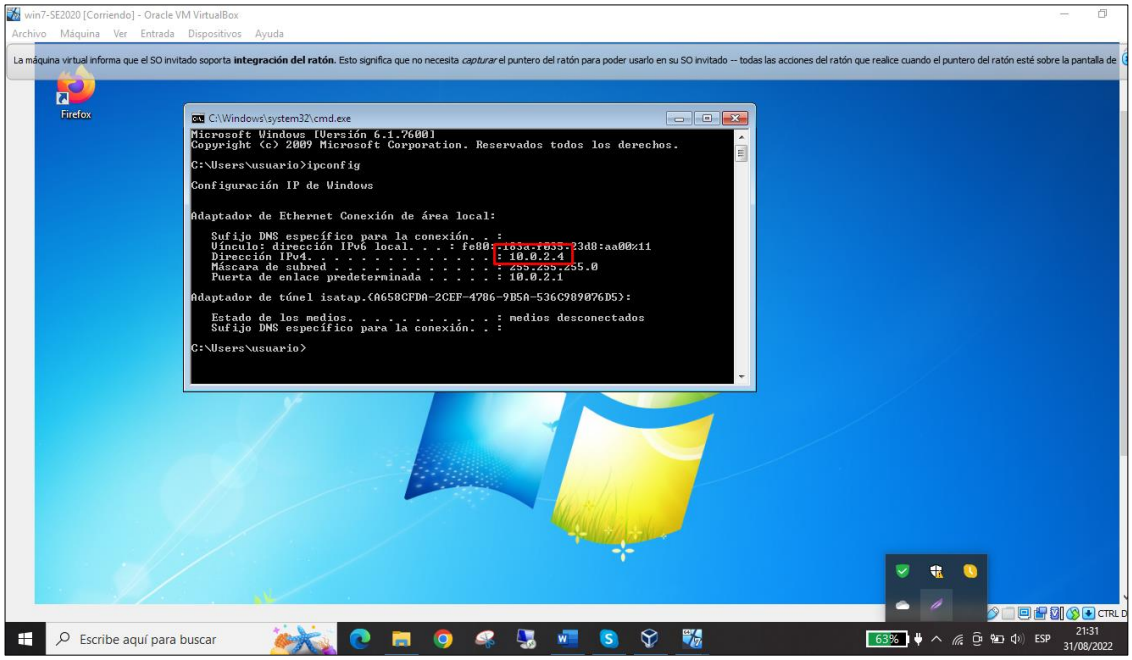


Fuente 2. Elaboración propia

Paso C. Comunicación de las maquinas Windows con la Linux

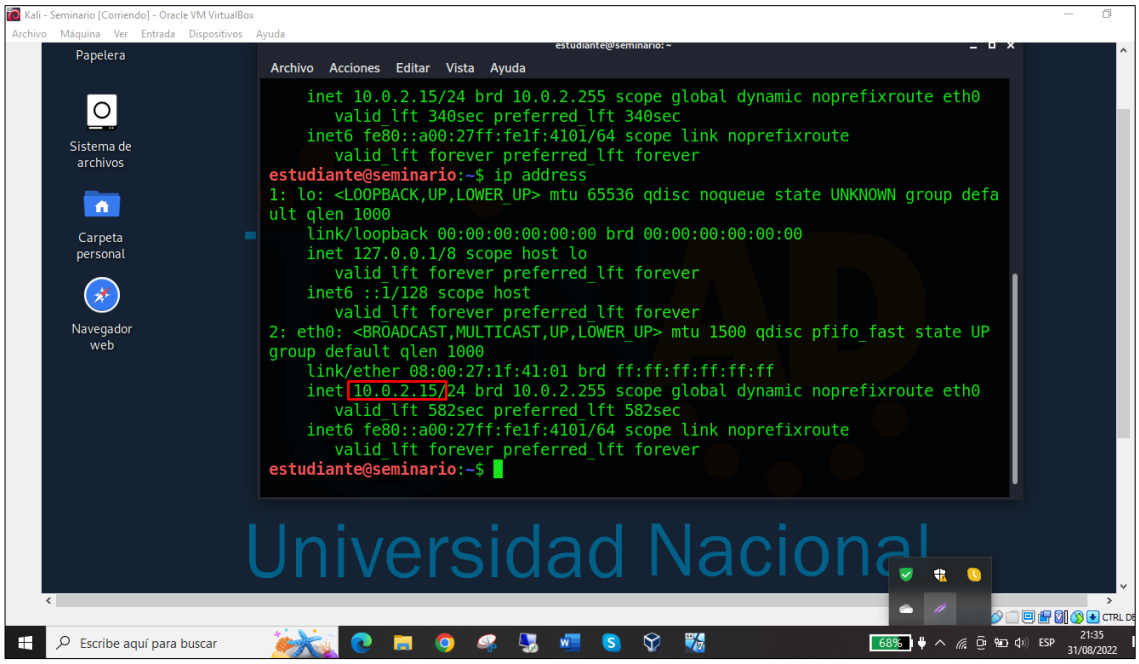
Primero vamos a conocer las IP´s de cada maquina:

Figura 3. Dirección IP de la maquina Win7 -SE2020



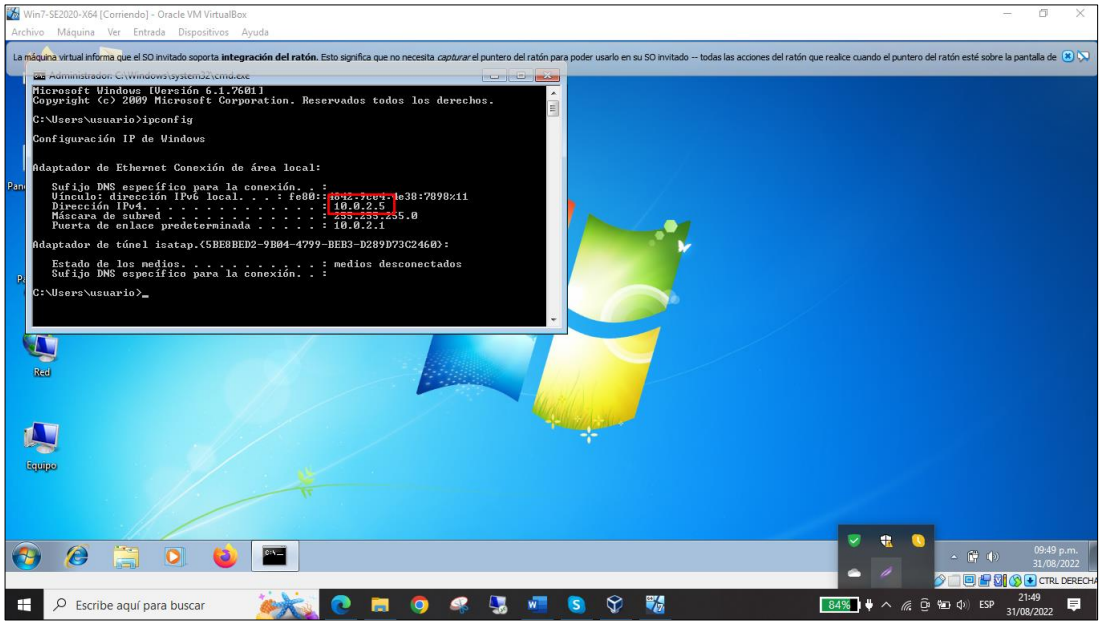
Fuente 3. Elaboración propia

Figura 4. Dirección IP de la maquina Kali



Fuente 4. Elaboración propia

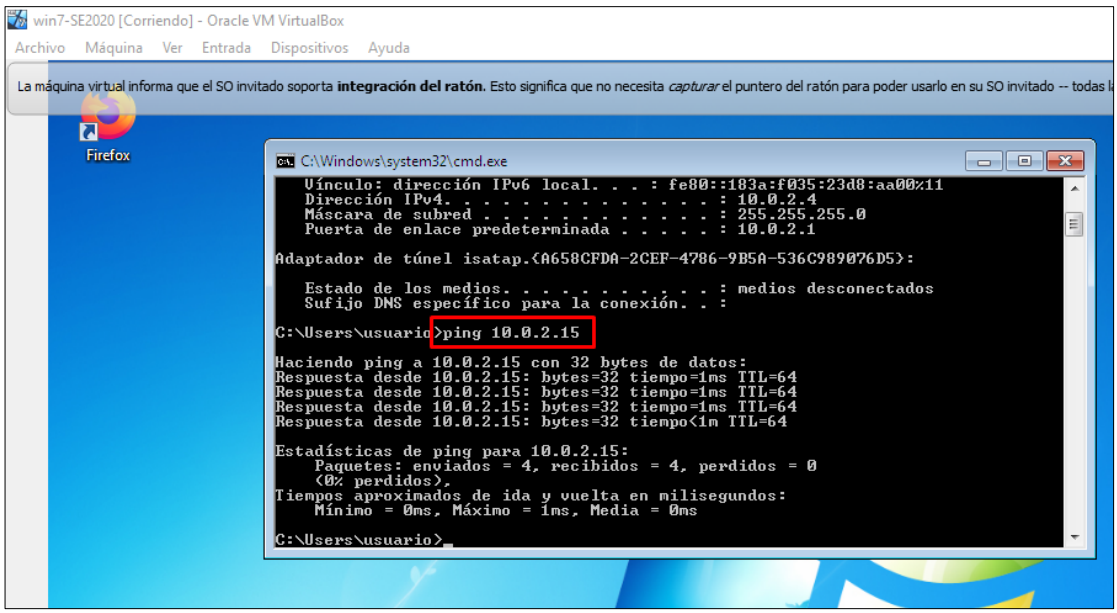
Figura 5. Elaboración IP de la maquina Win7 - SE2020 X64



Fuente 5. Elaboración propia

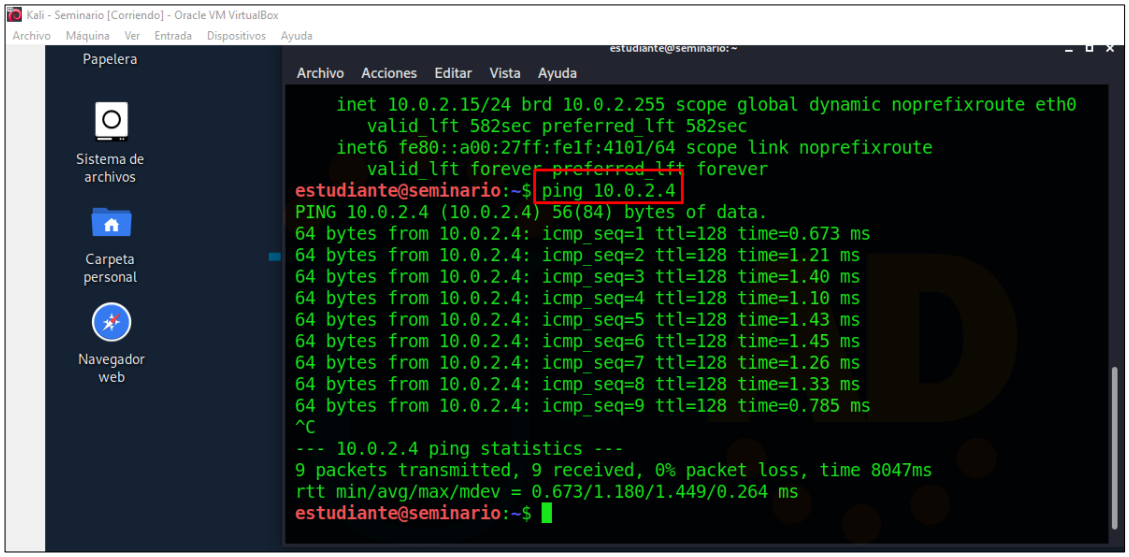
Luego procedemos a dar ping a la maquina Linux.

Figura 6. Ping de la maquina WIN7-SE2020 a la Kali



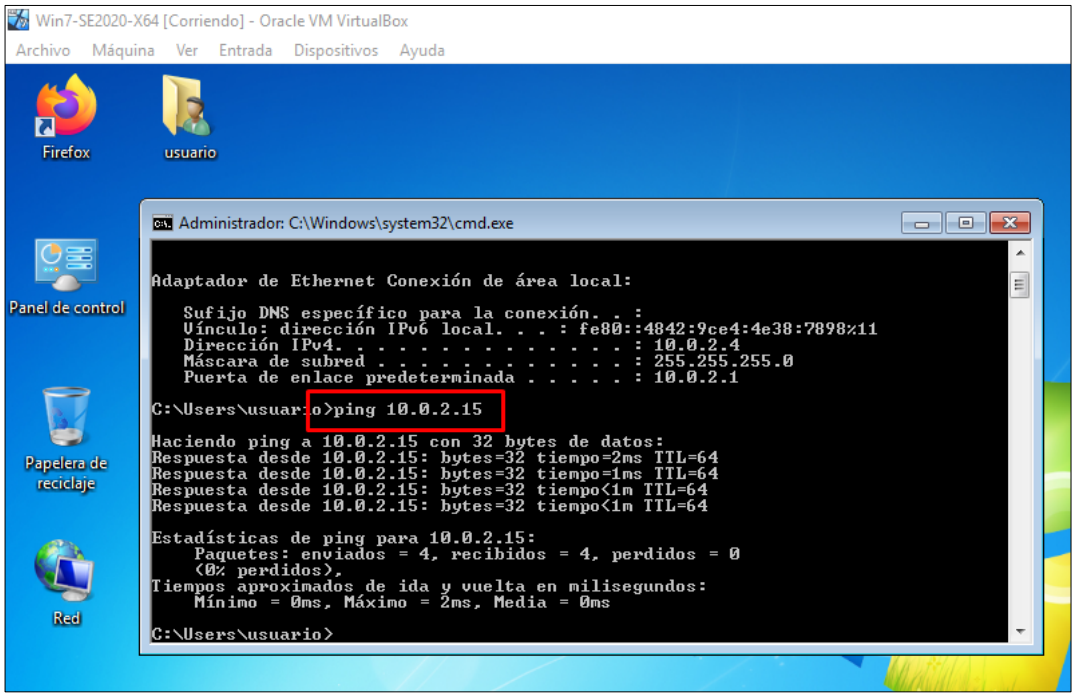
Fuente 6. Elaboración propia

Figura 7. Ping de la maquina Linux a la maquina WIN7-SE2020



Fuente 7. Elaboración propia

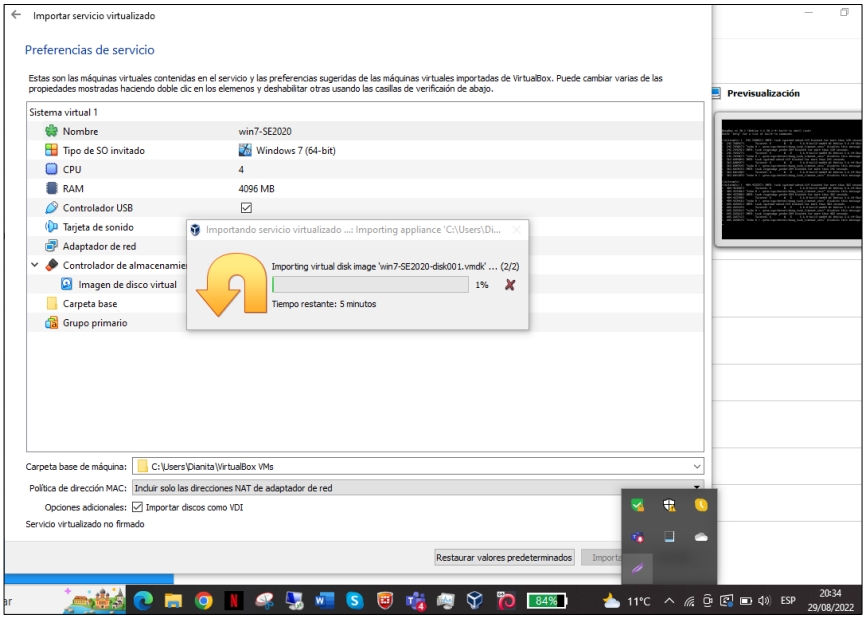
Figura 8. Ping de la maquina Win7 -SE2020 X64 a la Linux



Fuente 8. Elaboración propia

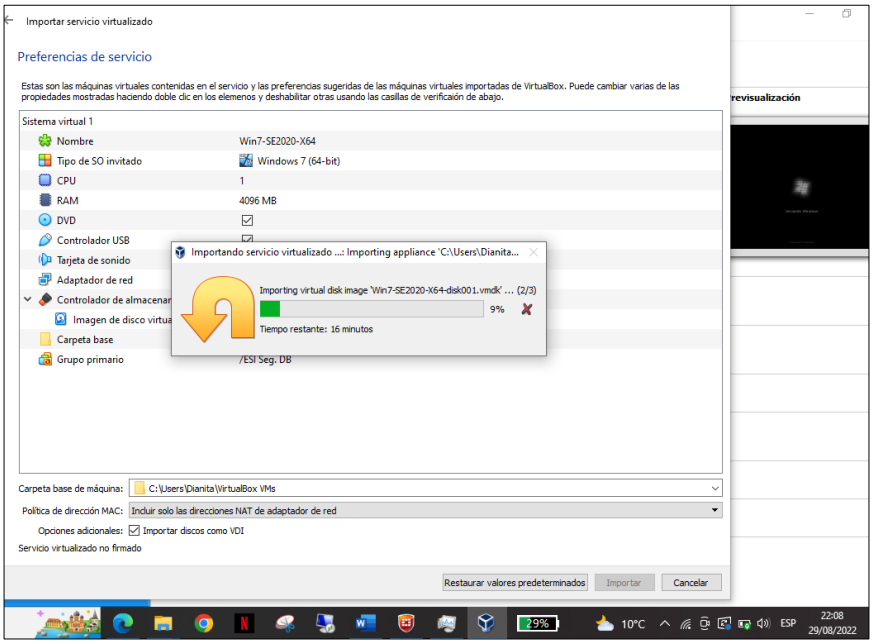
Paso D. Montaje del banco de trabajo

Figura 9. Importando maquina Win7-SE2020



Fuente 9. Elaboración propia

Figura 10. Importando maquina Win6 -SE2020 X64



Fuente 10. Elaboración propia

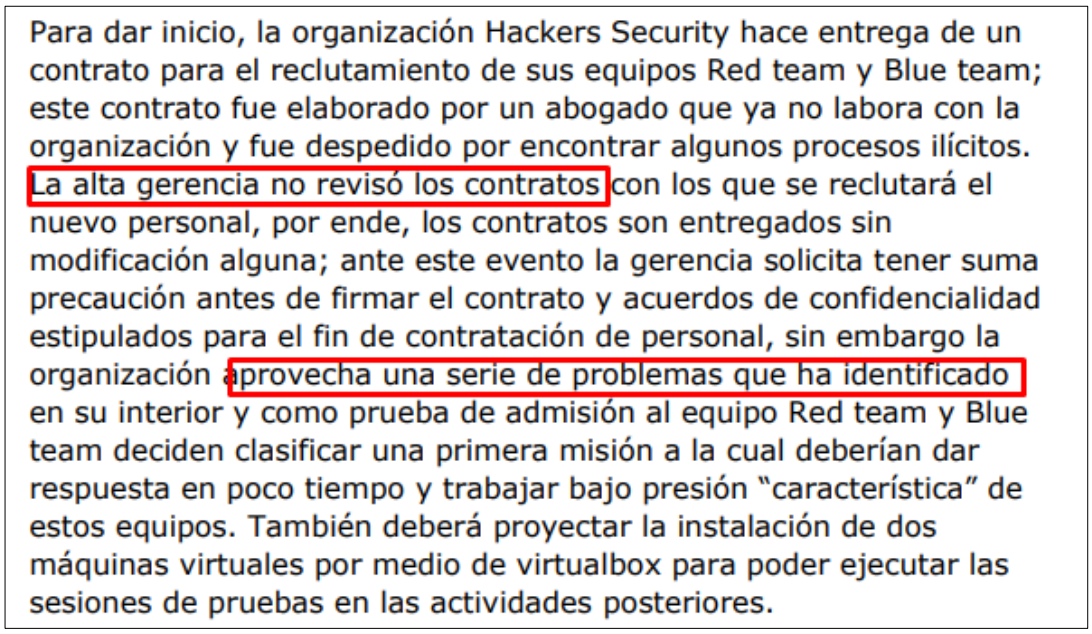
2.2 ETAPA 2 – ACTUACION ETICA Y LEGAL

En esta fase se evalúan los escenarios brindados indicando las posibles faltas de ética y procesos legales que se pueden evidenciar al momento de la contratación de los equipos de blue team y red team.

2.2.1 Lectura Anexo 2 y 3

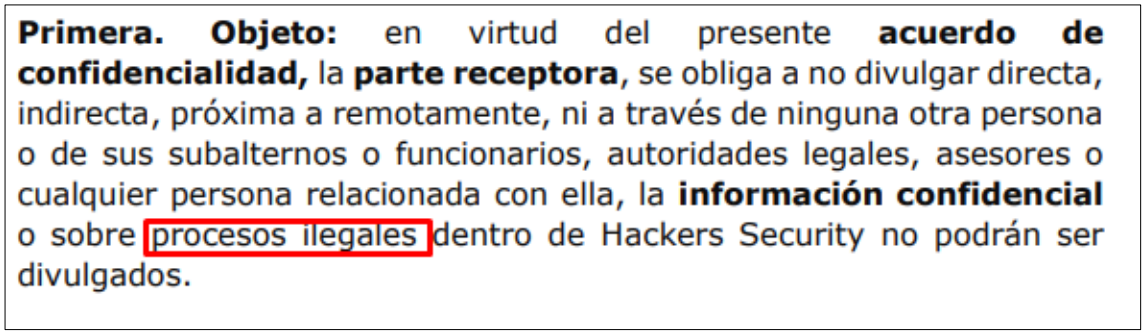
Como primer punto, la alta gerencia debió haber revisado los contratos para la contratación de los equipos de Blue Team y Red Team, y no aprovecharse de los incidentes ocasionados para que el grupo que estaban reclutando como prueba de admisión resolvieran el incidente sin haber estado contratados aprovechándose de la buena fe de las personas.

Figura 11. Captura del contrato sobre aprovecharse de las personas


Para dar inicio, la organización Hackers Security hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión "característica" de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores.

Fuente 11. Tomado de: Anexo 2 - Escenario 2

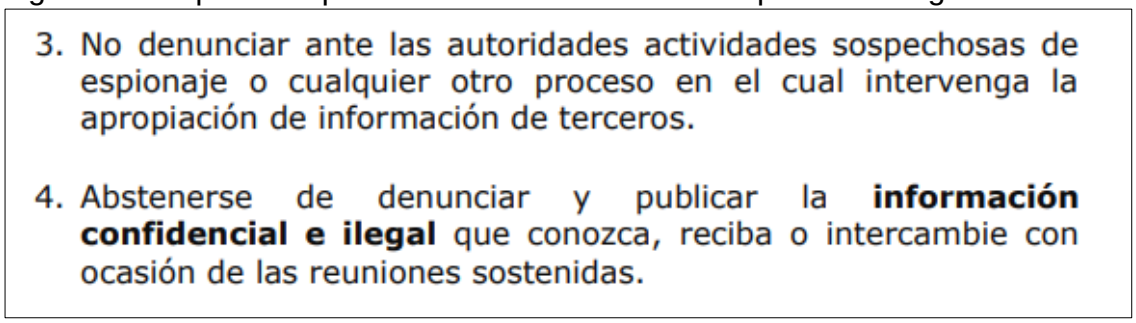
Figura 12. Captura del contrato sobre los procesos ilegales



Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la **información confidencial** o sobre procesos ilegales dentro de Hackers Security no podrán ser divulgados.

Fuente 12.Tomado de: Anexo 3 - Acuerdo

Figura 13. Captura de pantalla del contrato sobre los procesos ilegales



3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

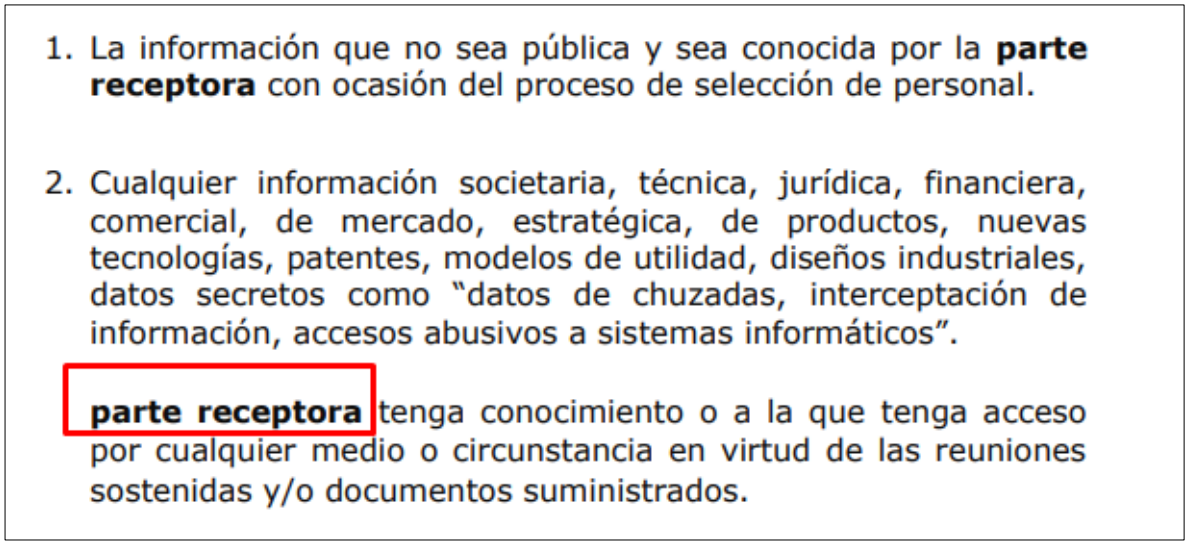
4. Abstenerse de denunciar y publicar la **información confidencial e ilegal** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

Fuente 13. Tomado de: Anexo 3 - Acuerdo

Según la figura No 2 y 3, se debe abstener de denunciar información ilegal sobre procesos y/o actividades ante las autoridades violando el Capitulo II Articulo 31 en el numeral F que indica que se debe denunciar todos los delitos que se tengan conocimiento[7].

[7] COPNIA. [Sitio web]. Código de ética. [Consulta: 10 de septiembre 2022]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Figura 14. Captura de pantalla del contrato con errores ortográficos



1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión del proceso de selección de personal.

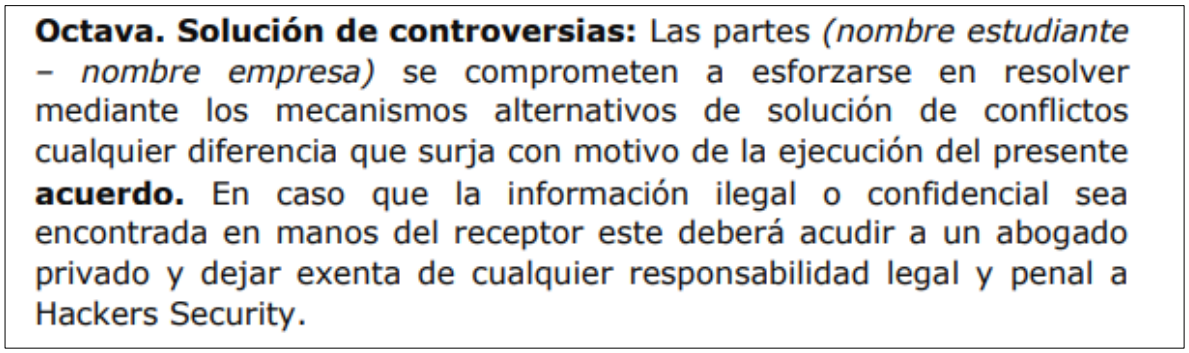
2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".

parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

Fuente 14. Tomado de: Anexo 3 – Acuerdo

Observando la figura 4 se puede determinar faltas de ortografía y espacio en blanco dentro del contrato.

Figura 15. Captura de pantalla del contrato sobre responsabilidad



Octava. Solución de controversias: Las partes *(nombre estudiante – nombre empresa)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Hackers Security.

Fuente 15. Tomado de: Anexo 3 - Acuerdo

No es ético y profesional que ante encontrarse con información ilegal, la persona deba acudir a un abogado externo y no comprometer de ninguna manera a la empresa asumiendo la evidencia. Esto no es nada correcto, ya que las actividades las realiza la organización y es quien debe hacerse cargo de lo que ocurra.

2.2.2 Artículos vulnerados en el acuerdo

Según la lectura se evidencian los siguientes artículos vulnerados:

Ley 1273: **Artículo 269A**
Articulo 269C
Articulo 269F

Estos artículos se están violando, ya que en el acuerdo indican que la parte receptora está obligada a no divulgar cualquier información ilegal que tenga conocimiento, como ejemplo acceso sin consentimiento a los sistemas (Artículo 269A) e interceptación de datos (Articulo 269C), datos de chuzadas y obtención ilegal de la información (Artículo 269F) [8].

2.2.3 Sueldo

No aceptaría la oferta ya que estaría violando el articulo 32 numeral B y F que indica que no se debe permitir ni tolerar el ejercicio ilegal de las profesiones y se debe denunciar esos delitos con las respectivas pruebas. Articulo 34 numeral a indica que no se deben aceptar trabajos en contra de las disposiciones legales.

Adicional que al incumplir los artículos que indica el código me estaría exponiendo según la gravedad de la infracción a que me cancelen la matricula profesional de por vida, que la suspendan por 5 años o la menor solo una amonestación escrita, por todas estas causales y porque al graduarse uno se compromete a colaborar con la sociedad reitero un NO a la oferta

[8] SUPERINTENDECIA INDUSTRIA Y COMERCIO. [Sitio web]. Ley 1273 de 2009. [Consulta: 11 de septiembre 2022]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

2.2.4 Operación Andrómeda Buggly

Aunque la operación Andrómeda fue legal, no hubo la correcta supervisión al personal asignado a esta misión, confiaron a ciegas tanto de los militares como del personal ajeno incumpliendo varios artículos de la ley 1273 para su beneficio personal, ya que estuvieron vendieron la información y no guardándola como es debido según el proceso por el cual fueron asignados. También aprovecharon las instalaciones para ejecutar el malware y poder capturar información de todos los computadores a los que fueron interceptados. Por ende la fiscalía tuvo que intervenir al validar que efectivamente las actividades que realizaban los militares no estaba siendo controlados correctamente. También los militares que formaron parte de ese grupo que infringió la ley fallaron en el código de ética ya que violaron varios artículos como recibir dinero intercambiando información ilegal.

2.3 ETAPA 3 – EJECUCION PRUEBAS

En esta etapa se evalúan los escenarios brindados logrando visualizar las vulnerabilidades que tiene el sistema a partir de técnicas y métodos de intrusión, demostrando el entorno a cargo de ReadTeam.

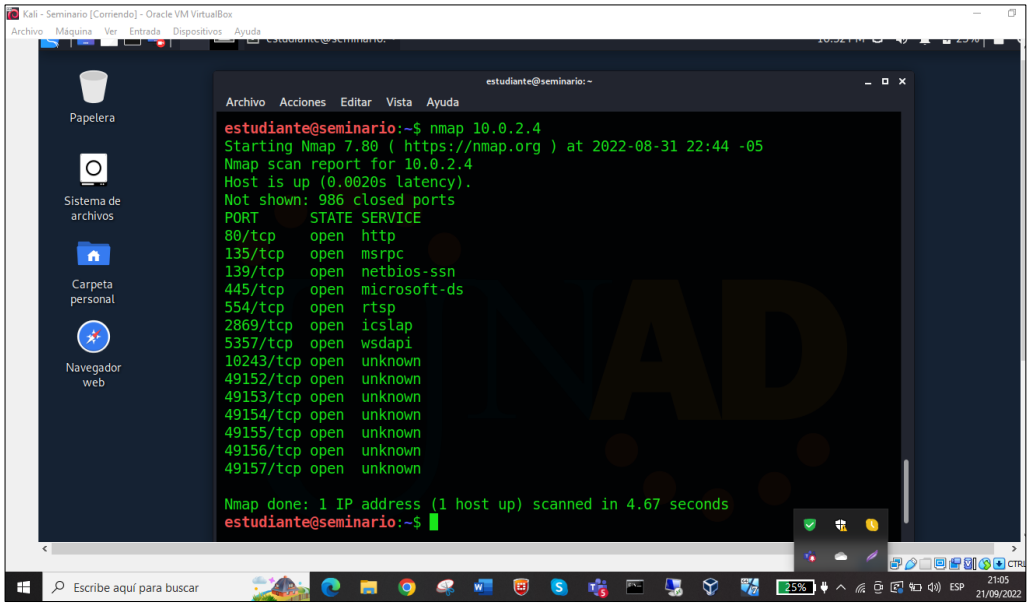
2.3.1 Herramientas de software utilizadas

Se utilizaron dos herramientas, la de NMAP que permite descubrir la red a atacar, nos permite conocer o rastrear los puertos abiertos para empezar a realizar ataques y evaluar la seguridad de esta. Aunque su función principal es la de trastear los puertos, NMAP permite validar aplicaciones, servidores, IP's entre otros[9]. Metasploit Framework es una herramienta que es especializada para las pruebas de los equipos Blue y Red que contiene diversidad de exploits para ser explotados.

Fase de recolección/reconocimiento:

[9] NMAP. [Sitio web]. Noticias. [Consulta: 20 de septiembre 2022]. Disponible en: https://nmap.org/

Figura 16. Nmap hacia la ip 10.0.2.4

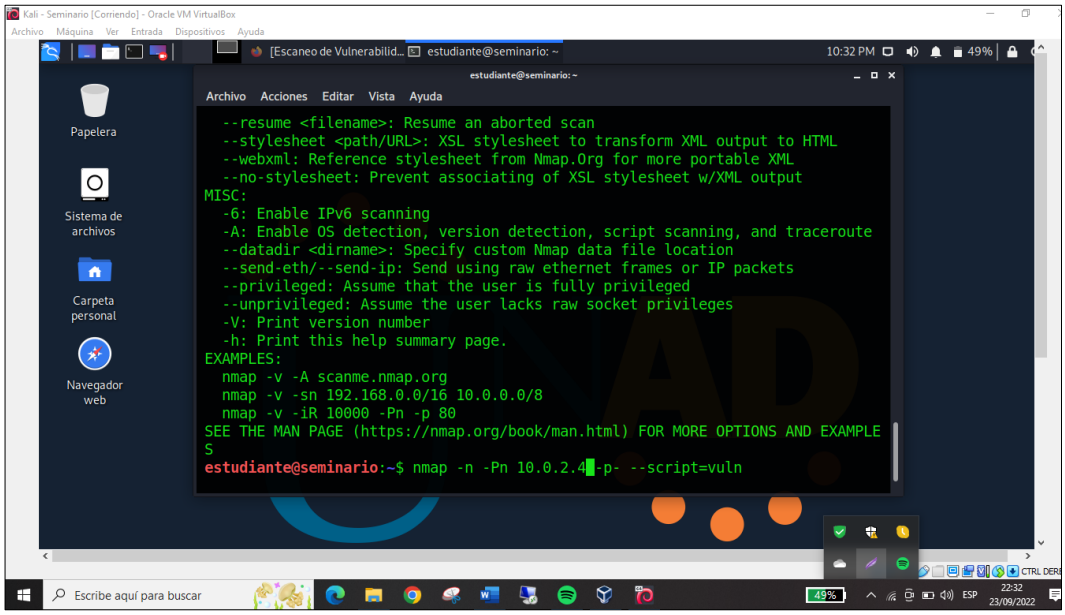


Fuente 16. Fuente propia

Se realiza un scaneo de puerto a la dirección 10.0.2.4

Fase de análisis de vulnerabilidades:

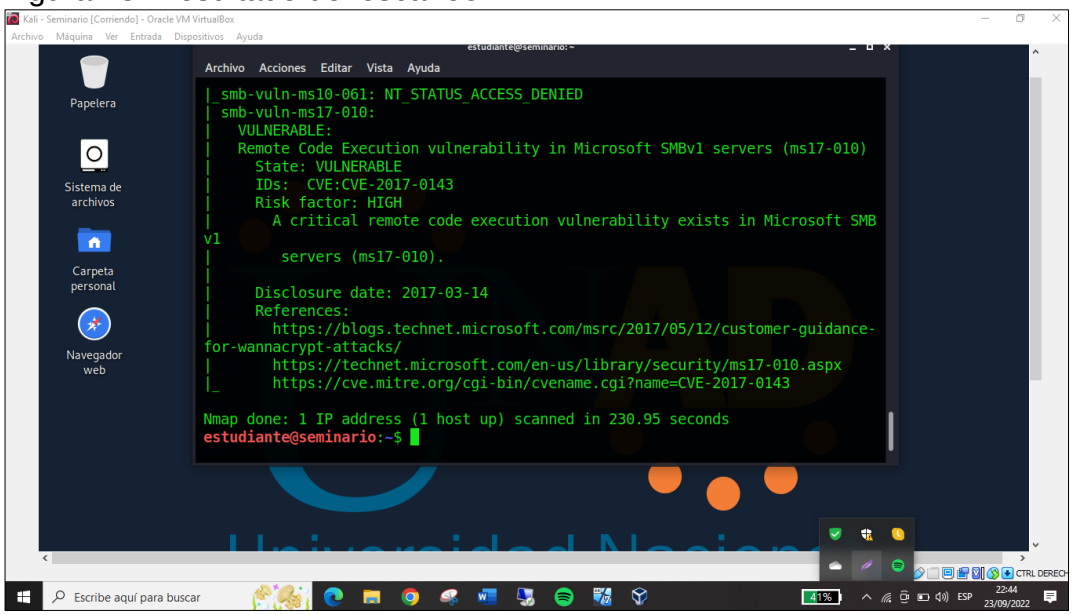
Figura 17. Comando para validar vulnerabilidades



Fuente 17.Fuente propia

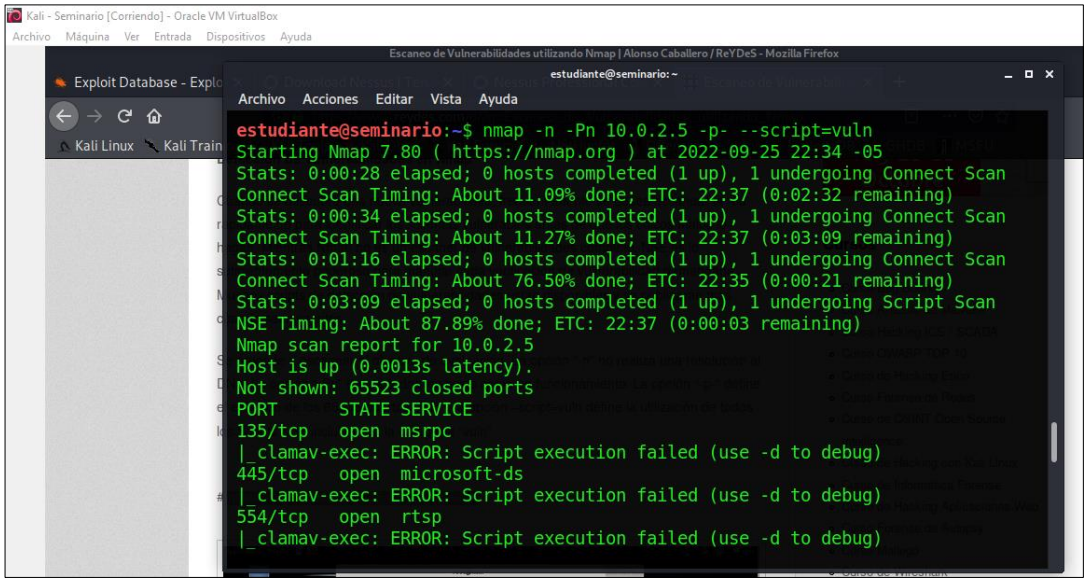
En la figura 2 se realiza el escaneo de vulnerabilidades hacia la ip 10.0.2.4 y en la figura 3 está el resultado del escaneo donde se permite visualizar la vulnerabilidad indicada

Figura 18. Resultado del escaneo



Fuente 18. Fuente propia

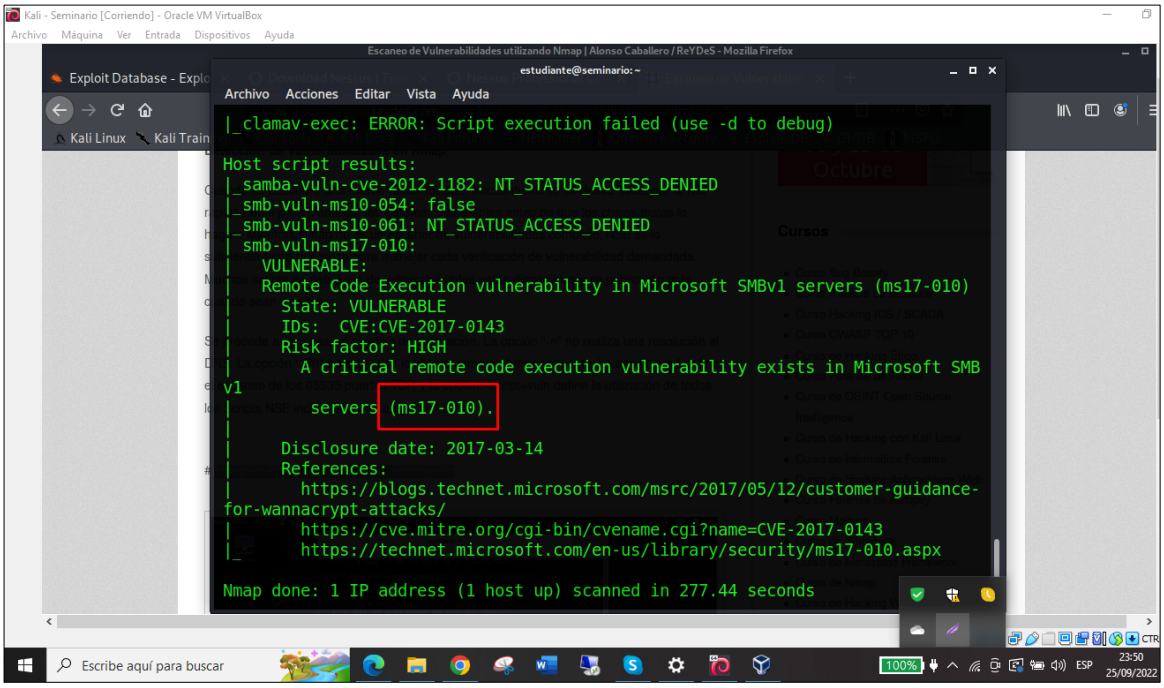
Figura 19. Scaneo de vulnerabilidades hacia la otra IP



Fuente 19. Fuente propia

En ambas maquinas Windows podemos encontrar la vulnerabilidad CVE 2017-0143

Figura 20. Resultado del escaneo de la otra maquina Windows



Fuente 20. Fuente propia

2.3.2 Fallo de seguridad Windows

- El equipo no contaba con sistema operativo actualizado y los parches no estaban aplicados a la fecha del incidente

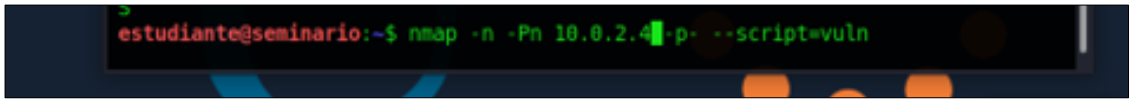
- Tener puertos abiertos que permiten realizar ataques con facilidad, contar con el protocolo SMB por el tema de la conexión de las impresoras

- Contar con el código CVE de la vulnerabilidad a explotar, ya que solo es buscar la forma en la web.

2.3.3 Herramientas para identificar fallos

Hay variedad de herramientas que nos permiten validar fallos de seguridad, la herramienta elegida para poder identificar los fallos fue la de **NMAP** con el comando nmap -n -Pn – IP -p - –script=vuln se puede visualizar las vulnerabilidades que tiene la IP

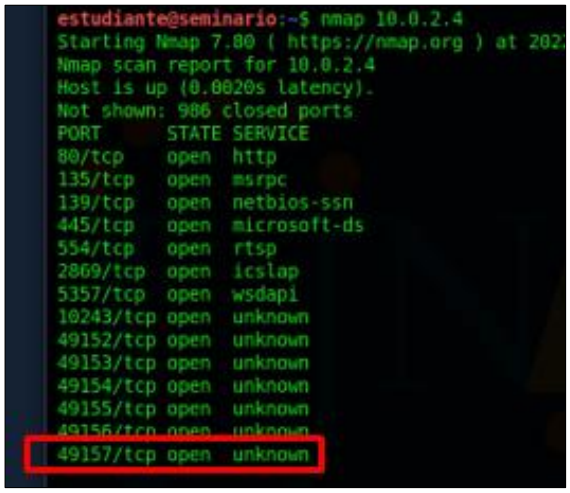
Figura 21. Comando para vulnerabilidades



Fuente 21. Elaboración propia

El puerto que abre la aplicación especifica es el 49157 el cual se encontraba abierto, en la primera fase al ejecutar NMAP este nos indicó que estaba abierto

Figura 22. Imagen donde se visualiza el puerto



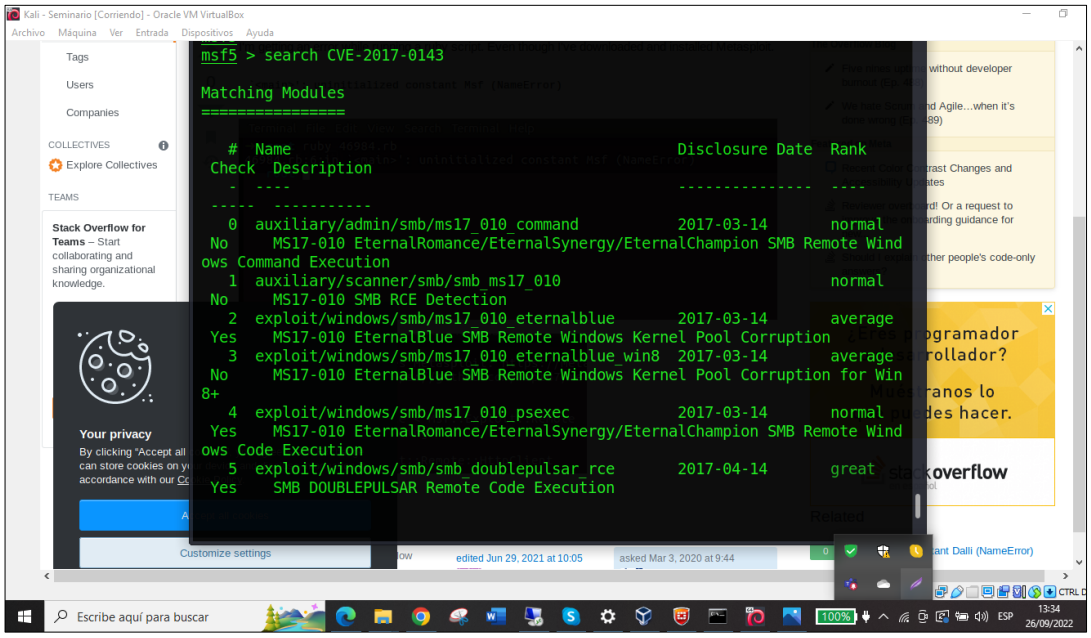
Fuente 22. Elaboración propia

2.3.4 Como afecta el ataque a la maquina

Este ataque afecta bastante a la maquina víctima, ya que permite tener acceso a la información y permite subir los privilegios para hacer un daño masivo con solo ejecutar el código en el servidor, por eso es muy importante contar con los parches / actualizaciones que nos brinda Microsoft.

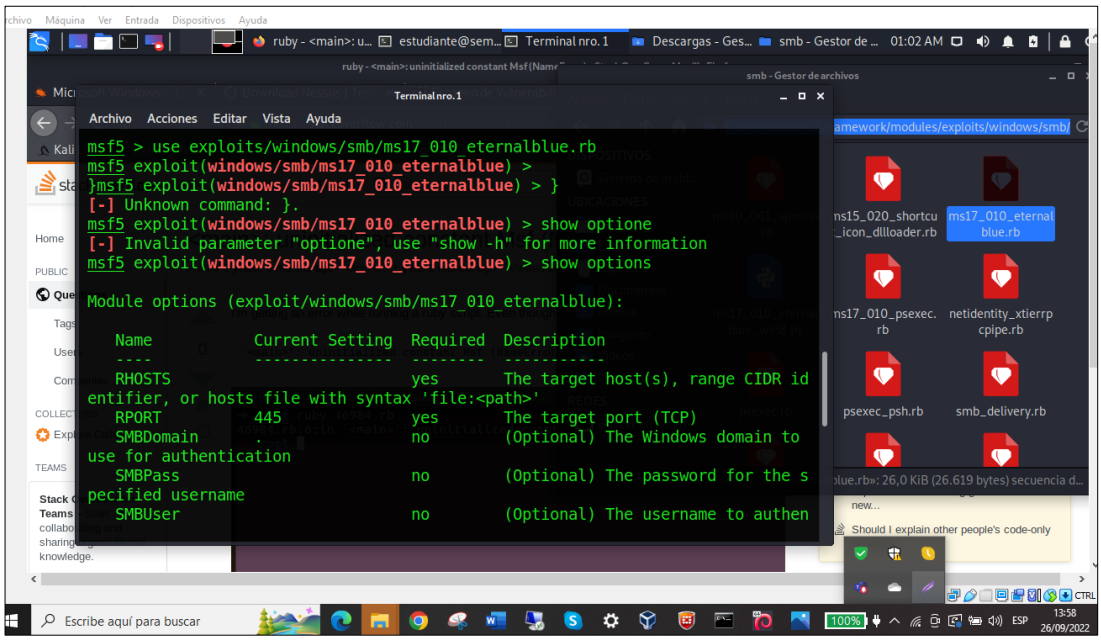
2.3.5 Evidencias

Figura 23. Buscando el CVE en Metasploitable



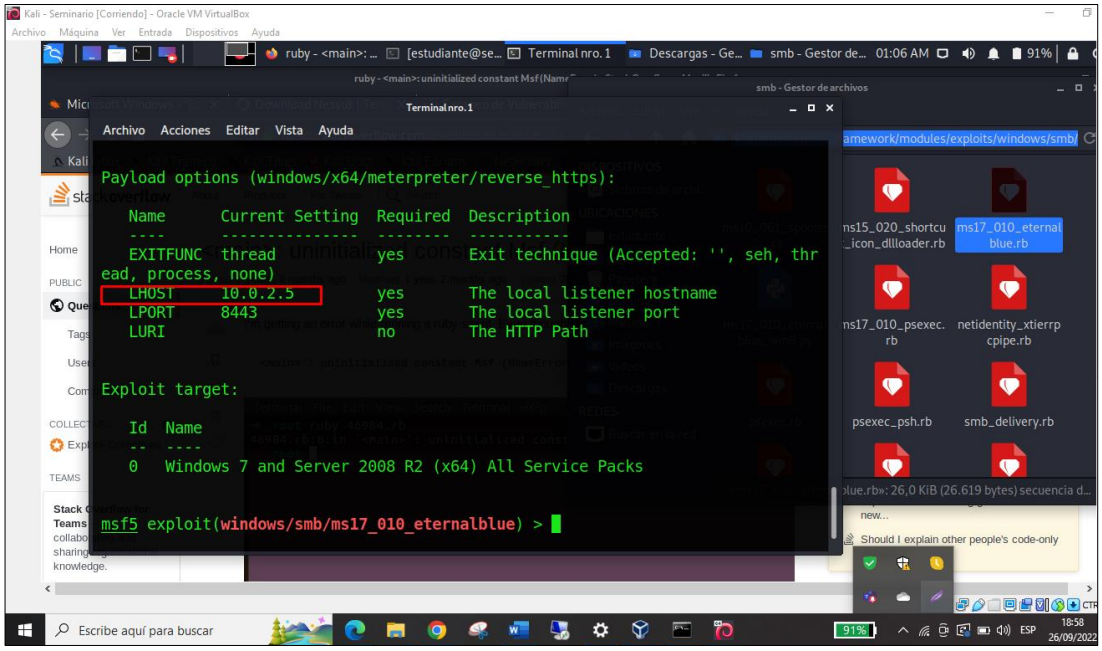
Fuente 23. Elaboración propia

Figura 24. Encontrando la opción del exploit



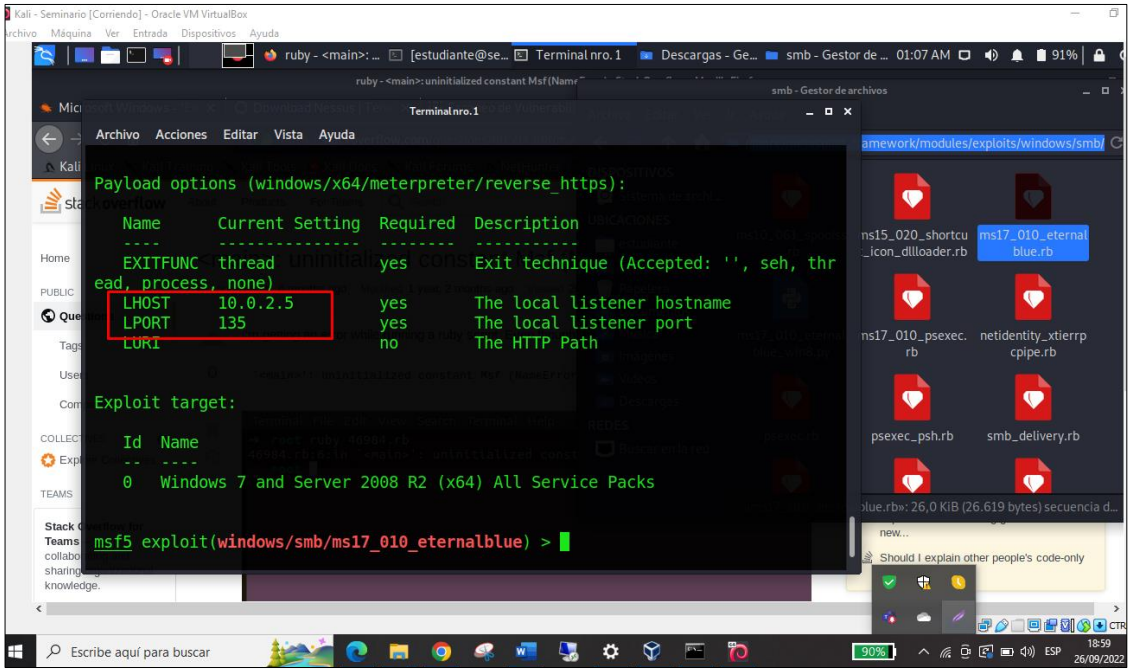
Fuente 24. Elaboración propia

Figura 25. Modificando los parámetros



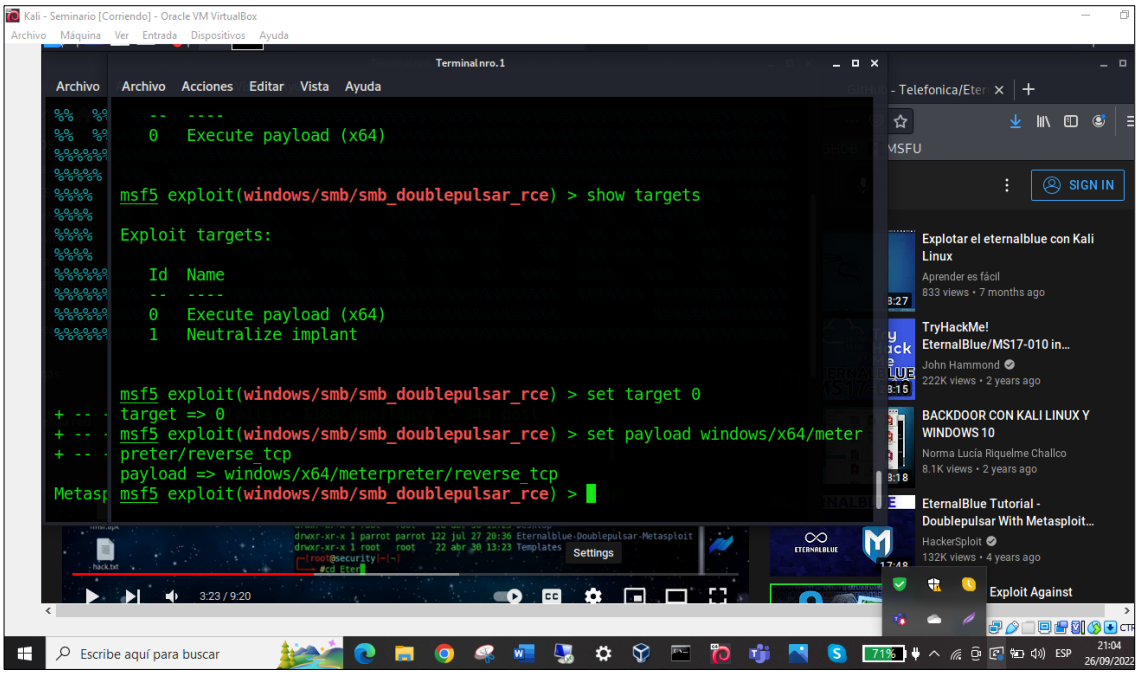
Fuente 25. Elaboración propia

Figura 26. Parámetros configurados para el exploit



Fuente 26. Elaboración propia

Figura 27. Modificación de targets



Fuente 27. Elaboración propia

2.4 ETAPA 4 – CONTENCION DE ATAQUES

En esta etapa se evalúan los escenarios brindados logrando formular estrategias que permitan contener un ataque y minimizar los daños al mismo, mediante el análisis de riesgos y vulnerabilidades.

2.4.1 Acciones durante un ataque real

Lo primero que realizaría es tratar de identificar qué tipo de ataque se está presentando, para así poder buscar la mejor forma de disminuir el impacto del ataque, nos podemos basar en el plan de acción propuesto por Deloitte legal que consiste en 4 fases[10]:

[10] DELOITTE. [Sitio web]. Pasos a seguir ante un ataque informático. [Consulta: 03 de octubre 2022]. Disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

La primera es la fase de prevención: Consiste en generar medidas preventivas en la organización para poder hacer en el entorno más difícil de penetrar para un hacker. Desde definir los roles y matrices para consultar la información hasta el control de dispositivos extraíbles.

La segunda es la fase de detección: Esta fase es muy importante ya que dependiendo de la gestión que se realice, se puede lograr a disminuir considerablemente el impacto que el ataque nos genere basándonos en medidas organizativas como legales.

La tercera es la fase de recuperación: En esta fase la idea es lograr recuperar la operación de la empresa después de un ataque, para todo esto es muy importante contar con un plan de continuidad del negocio, que consiste en contemplar cualquier situación que pueda poner en riesgo a la empresa, logrando recuperarse después del impacto, desde generar copias de seguridad hasta el backup de los sistemas con que se cuenten.

La cuarta es la fase de respuesta: En esta fase la idea es informar a todo el personal involucrado con la empresa, desde los clientes, proveedores hasta los mismos trabadores con el fin de disminuir la información sustraída.

2.4.2 Medidas de Hardenización

Según el ejercicio realizado en la anterior actividad, las medidas de hardenización que se contemplarían son[11]:

- Cambio de usuarios y claves que se tengan por defecto
- Contraseñas robustas
- Cerrar puertos que no sean necesarios

[11] CISET. . [Sitio web]. ¿Qué es el hardening de sistemas operativos? [Consulta: 03 de octubre 2022]. Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening

- Instalar Firewall tanto en servidores como equipos de computo
- Estar al día en parches de seguridad
- Contar con herramienta de escaneo de vulnerabilidades
- Implementar un DLP para la fuga de información

2.4.3 Diferencias entre un equipo Blue Team y un equipo de respuesta

Un equipo de respuesta a los incidentes tiene como objetivo recibir, revisar y responder de forma inmediata a los incidentes[12], mientras que el objetivo del Blue Team es generar las evaluaciones de la variedad de amenazas que pueden afectar para poder mitigar los riesgos encontrados.

La función de un equipo de respuesta es lograr salvaguardar el sistema y preservar la información de la organización, esto con base a los incidentes que pasan a nivel mundial logrando generar entre varios equipos de respuestas excelentes estrategias y las funciones de un equipo de Blue Team son trabajar en la mejora día a día de la seguridad y realizar vigilancia, analizando los patrones encontrados[13].

El equipo Blue Team está conformado por expertos en seguridad informática y el equipo de incidentes puede ser tanto externo como interno entrenados para responder con rapidez reduciendo tiempo y costos de recuperación.

2.4.4 Utilizar CIS

Lo utilizaría para poder defender el sistema de la empresa, ya que CIS se refiere a los controles de Seguridad Critica, y este nos provee las mejores prácticas para la defensa cibernética orientándonos de una manera específica para poder lograr la meta bajo diferentes marcos.

---

[12] SECURITY ADVISOR. Sitio web]. ¿Qué es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT? [Consulta: 03 de octubre 2022]. Disponible en: https://sadvisor.com/que-es-el-csirt/

[13] TECHTARGET. Sitio web]. CERT vs. CSIRT vs. SOC: What's the difference? [Consulta: 03 de octubre 2022]. Disponible en: https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

2.4.5 Que es un SIEM

Un SIEM es un sistema que es capaz de detectar, responder y neutralizar ante eventos, incidentes en los sistemas de las organizaciones. Este tiene un aprendizaje inicial que al detectar un patrón fuera del inicial, actúa de forma inmediata, el SIEM es la evolución del SEM y del SIM[14]. El SIEM registra los logs permitiendo que se puedan realizar los análisis en tiempo real. La función principal de un SIEM es detectar y prevenir amenazas. Sus principales características son:

- Reconocer entre incidentes falsos y amenazas reales
- Registrar y documentar todo el proceso de detección y la resolución
- Tiempos de respuesta
- Análisis e investigación

Beneficios de un SIEM[15]:

- Respuesta automática a eventos
- Información rápida y eficiente
- Seguimiento de eventos
- Deteccion de violaciones de seguridad
- Mejor manejo del riesgo

Algunas herramientas que nos ofrecen esto son:

IBM Security QRadar, McAfee Enterprise Security Manager, LogRhythm entre otras.

2.4.6 Definición de herramientas de contención de ataques

[14] AMBIT. [Sitio web]. ¿Qué significa SIEM y cómo funciona? [Consulta: 01 de octubre 2022]. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona#

[15] NSIT. [Sitio web]. ¿Qué es SIEM en seguridad informática? Alcance e implementación [Consulta: 02 de octubre 2022]. Disponible en: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

Antivirus: El antivirus es una herramienta bastante robusta que nos permite proteger y contener un ataque, ya que este bloquea o envía a cuarentena cualquier archivo que encuentre sospechoso para la organización.

Firewall: El firewall nos permite bloquear cualquier IP que se encuentre reportada como maliciosa, si nos intentan atacar, este realiza la protección debida y nos reporta el ataque.

Full Disk Encryption: Ante un intento de robar la información de un equipo, el contar con esta herramienta no permite al atacante extraer la información, solo le queda formatear el equipo para reutilizar.

Email Security: Ante un ataque de archivos y/o extensiones peligrosas, esta herramienta nos permite bloquear los adjuntos o el correo completo para así evitar que al abrirlo se expanda un virus

3 RECOMENDACIONES

Las recomendaciones para *Hackers Security* *son las siguientes*:

- Se debe implementar herramientas de IDS/IPS que permitan proteger los sistemas de detección y prevención de intrusos, monitoreando el tráfico, alertando y bloqueando cualquier movimiento inusual que detecte.

- Se debe implementar un firewall que permita impedir que los atacantes externos puedan acceder al sistema, supervisando el tráfico de red y bloqueando el tráfico no reconocido.

- El director de tecnología debe implementar pruebas de vulnerabilidades por lo menos 2 veces al año para ir mitigando según los resultados

- Los usuarios de seguridad deben implementar un antivirus que les permita proteger tanto los servidores como los equipos de cómputo de virus informáticos que se puedan generar y/o filtrar por medio de USB permitidas o por canales externos

- El personal de seguridad debe implementar una solución Antispam respectivamente configurada para asegurar que los correos que lleguen sea legítimos y no ingrese ningún tipo de virus.

4 CONCLUSIONES

Según el trabajo entregado se concluye que es importante en las empresas contar con un equipo de respuesta a los incidentes, ya que con esto garantizamos que el retorno a las actividades normales de la empresa es más rápido de lo normal.

Al ingresar a un nuevo empleo es recomendable validar efectivamente lo que indica el contrato y si se tienen dudas al respecto es mejor hacerlas saber y no aceptar cosas que después se estén arrepintiendo.

Contar con una buena herramienta tanto para la recolección como para la explotación de las vulnerabilidades es primordial para poder llevar a cabo el ataque con éxito

BIBLIOGRAFÍA

AMBIT. [Sitio web]. ¿Qué significa SIEM y cómo funciona? [Consulta: 01 de octubre 2022]. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona#

COPNIA. [Sitio web]. Código de ética. [Consulta: 10 de septiembre 2022]. Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

CISET. . [Sitio web]. ¿Qué es el hardening de sistemas operativos? [Consulta: 03 de octubre 2022]. Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening

DELOITTE. [Sitio web]. Pasos a seguir ante un ataque informático. [Consulta: 03 de octubre 2022]. Disponible en: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html

HOSTING PLUS. [Sitio web]. Qué es Metasploit framework. [Consulta: 03 de septiembre 2022]. Disponible en: https://www.hostingplus.com.co/blog/que-es-nmap-y-para-que-sirve/

LIU, Simon; KUHN, Rick. Data loss prevention. IT professional, 2010, vol. 12, no 2, p. 7

NMAP. [Sitio web]. Noticias. [Consulta: 20 de septiembre 2022]. Disponible en: https://nmap.org/

NSIT. [Sitio web]. ¿Qué es SIEM en seguridad informática? Alcance e implementación [Consulta: 02 de octubre 2022]. Disponible en: https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/

OPEN WEBINARS. [Sitio web]. Qué es Metasploit framework. [Consulta: 02 de septiembre 2022]. Disponible en: https://openwebinars.net/blog/que-es-metasploit/

OPEN WEBINARS . [Sitio web]. Qué es OpenVas? [Consulta: 03 de septiembre 2022]. Disponible en: https://openwebinars.net/blog/que-es-openvas/

POLICIA NACIONAL DE COLOMBIA. [Sitio web]. Normatividad sobre delitos informáticos. [Consulta: 01 de septiembre 2022]. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

SECURITY ADVISOR. Sitio web]. ¿Qué es el Equipo de Respuesta ante Incidentes de Seguridad Informática CSIRT? [Consulta: 03 de octubre 2022]. Disponible en: https://sadvisor.com/que-es-el-csirt/

SUPERINTENDECIA INDUSTRIA Y COMERCIO. . [Sitio web]. Protección de Datos Personales. [Consulta: 01 de septiembre 2022]. Disponible en: https://www.sic.gov.co/preguntas-frecuentes-pdp#:~:text=La%20Ley%201581%20de%202012%20proh%C3%ADbe%20la%20transferencia%20de%20datos,e%20inequ%C3%ADvoca%20para%20la%20transferencia.

SUPERINTENDECIA INDUSTRIA Y COMERCIO. [Sitio web]. Ley 1273 de 2009. [Consulta: 11 de septiembre 2022]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

TECHTARGET. Sitio web]. CERT vs. CSIRT vs. SOC: What's the difference? [Consulta: 03 de octubre 2022]. Disponible en: https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

ANEXOS

ANEXO A

Link de video: https://youtu.be/fbs-I6P7FGE

ANEXO B